UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,859	02/01/2007	Brijbhushan S. Sabnis	A8598	4207

23373 7590 07/03/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/573,859	SABNIS ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/29/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on March 29, 2006.

2. Claims 1-16 are under examination.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on March 29, 2006. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

4. The specification filed March 29, 2006 is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d) (1) and MPEP § 608.01 (o). Correction of the following is required: the term "computer readable medium" in claims 9-12 doesn't have antecedent basis in the specification.

Claim Objections

5. Claims 1 and 9 are objected to because of the following informalities:

Claim 1 recites the limitations **"the certification path"**, is objected for lacking proper antecedent basis. Examiner is interpreted as "a certification path".

Claim 9 is objected for the preamble which recites the limitation "A **computer readable medium of program** instruction ….". Appropriate preamble should recite "A computer readable medium storing program instruction .....".

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-4 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1 recites "A digital certificate, comprising: a *distinguished name (DN) field*; and *a common name (CN) field* within the DN field, containing a resource identifier, wherein the resource identifier contains information identifying each of a plurality of certificate-issuing resources in the certification path of the digital certificate". Claim 1 recites limitation that is merely arrangement of data and thus does not fall within the statutory category listed in 35 USC § 101. Further, the arrangement of data is nonfunctional descriptive material per se. Therefore, claim 1 **recites non-statutory subject matter**.

Claims 2-4 depend on claim 1, therefore they are rejected with the same rationale applied against claim 1 above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Benantar et al (US Pub. No. 2003/0065920) and in view of Perlman (US Pub. No. 2002/0147905).

As per claim 1, Benantar teaches:

A digital certificate **[Fig. 5, 500]**, comprising: a distinguished name (DN) field **[Fig. 5, 506]**; and a common name (CN) field within the DN field **[paragraph 0032, lines 18-28 "The distinguished name (DN) of a subject or issuer is formed by concatenating a series of relative distinguished name (RDNs) corresponding to nodes in a tree known as a directory information tree (DIT). Thus, the distinguished name CN=John Doe, OU=Research, O=Widgets.com, C=US is the concatenation (beginning from the root of the tree) of the RDNs C=US, O=Widgets.com, OU=Research and CN=John Doe, where C signifies country, O signifies organization, OU signifies organizational unit, and CN signifies common name", Fig. 5]**. Benantar teaches the common name field within the distinguished name field, containing a resource identifier (e.g. identifying information) identifying each of a plurality of resources in a tree **[paragraph 0032 lines 18-22, "The distinguished name (DN) of a subject or issuer is formed by concatenating a series of relative distinguished name (RDNs) corresponding to nodes in a tree known as a directory information tree (DIT)].** Benantar doesn't explicitly mention identifying *each*

of a plurality of certificate-issuing resources in the certification path of the digital certificate.

However, Perlman teaches: the digital certificate **[Fig. 5, 4]** contains the identifying information identifying each of a plurality of certificate-issuing resources in a certification path of the digital certificate **[Fig. 5, 3, paragraph 0036, "Certificate chains generated by CA's in conventional systems typically comprise certificate chains like the certificate chain 40. For example, in the event the top-down model 30 is deployed in a conventional system....", paragraph 0037, a conventional certificate chain comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N), and an indication 56 of the identity of a client", paragraph 0051].**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the digital certificate of Benantar's invention by including the identification information as taught by Perlman because it would reduce bandwidth utilization and processing overhead associated with the processing of linked certificates **[Perlman, paragraph 0021 lines 6-11].**

As per claim 2, the rejection of claim 1 is incorporated and Perlman teaches:

the resource identifier is a hierarchical identifier specifying an identity of a trusted root resource, and an identity of a resource issuing the digital certificate **[Fig. 3, 5, paragraph 0029 "FIG. 3 depicts an exemplary Public Key Infrastructure (PKI) model 30, which may be deployed in the computer network 16 (see FIG. 1) to enable the discovery of public keys. Specifically, the PKI model 30 comprises a "top-down" hierarchical model that includes a single root CA 14.1, a plurality of Intermediate Certification Authorities (ICA's) 14.2-14.7", paragraph 0030 " In the top-down model 30, each of the clients 12.1-12.4 trusts the root CA 14.1.", paragraph 0037 "a conventional certificate chain comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N)"].**

As per claim 3, the rejection of claim 1 is incorporated and Perlman teaches:

the resource identifier further contains identifiers of certificate-issuing resources in a certification path between the trusted root resource and the resource issuing the digital certificate [Fig. 3, 5, **paragraph 0029, paragraph 0037 "a conventional certificate chain comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one**

embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N)", paragraph 0050, 0051 "the root CA 14.1 may generate a collapsed certificate for the ICA 14.5 signed by the root CA 14.1 and including an indication of the identity of the ICA 14.4. Similarly, the ICA 14.4 may generate a collapsed certificate for the client 12.3 signed by the ICA 14.4 and including an indication of the identity of the ICA 14.5. Accordingly, consistent with the present invention, a collapsed certificate may be generated anywhere within a chain of linked certificates, in which two (2) or more linked certificates are collapsed to form a single certificate"].

As per claim 4, the rejection of claim 1 is incorporated and Benantar teaches the digital certificate is for use in a computing system **[Figs. 1, 3, 4]**. Further, Perlman teaches the digital certificate is for use in a computing system, and the certification path leads to a trusted source for the computing system **[Figs. 1-3, paragraph 0023 "The system 10 includes a plurality of entities. In this illustrative embodiment, such entities may comprise components in a computer network such as principals, clients, servers", paragraph 0024 "the system 10 includes a plurality of clients 12.1-12.N, a plurality of Certification Authorities (CA's) 14.1-14.N, a Directory Server (DS) 18 operative to provide access to certificates issued by one or more of the CA's 14", paragraph 0029 "Public Key Infrastructure (PKI) model 30, which may be deployed in the computer network 16 (see FIG. 1) to**

enable the discovery of public keys. Specifically, the PKI model 30 comprises a "top-down" hierarchical model that includes a single root CA 14.1, a plurality of Intermediate Certification Authorities (ICA's) 14.2-14.7, and a plurality of clients 12.1-12.4", paragraph 0030].

As per claim 5, Benantar teaches:

A method for generating a digital certificate with an authority identification field **[Fig. 5, 500]**, comprising: signing the digital certificate **[Fig. 5, 508];** inserting into the authority identification field a resource identifier that contains information identifying certificate-issuing resource **[Fig. 506].** Benantar teaches the authority identification field, contains identifying information identifying each of a plurality of resources in a tree **[paragraph 0032 lines 18-22, "The distinguished name (DN) of a subject or issuer is formed by concatenating a series of relative distinguished name (RDNs) corresponding to nodes in a tree known as a directory information tree (DIT)].** Benantar doesn't explicitly mention identifying *each of a plurality of certificate-issuing resources in the certification path of the digital certificate*.

However, Perlman teaches: the digital certificate **[Fig. 5, 4]** contains the identifying information identifying *each of a plurality of certificate-issuing resources in a certification path of the digital certificate* **[Fig. 5, 3, paragraph 0036, "Certificate chains generated by CA's in conventional systems typically comprise certificate chains like the certificate chain 40. For example, in the event the top-down model 30 is deployed in a conventional system....", paragraph 0037, a conventional certificate chain**

comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N), and an indication 56 of the identity of a client", paragraph 0051].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the digital certificate of Benantar's invention by including the identification information as taught by Perlman because it would reduce bandwidth utilization and processing overhead associated with the processing of linked certificates **[Perlman, paragraph 0021 lines 6-11].**

As per claim 6, the rejection of claim 5 is incorporated and Perlman teaches:

the resource identifier is a hierarchical identifier specifying an identity of a trusted root resource, and an identity of a resource issuing the digital certificate **[Fig. 3, 5, paragraph 0029 "FIG. 3 depicts an exemplary Public Key Infrastructure (PKI) model 30, which may be deployed in the computer network 16 (see FIG. 1) to enable the discovery of public keys. Specifically, the PKI model 30 comprises a "top-down" hierarchical model that includes a single root CA 14.1, a plurality of Intermediate Certification Authorities (ICA's) 14.2-14.7", paragraph 0030 " In the top-down model 30, each of the clients 12.1-12.4 trusts the root CA 14.1.", paragraph 0037 "a conventional certificate chain comprising a plurality of linked**

certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N)"].

As per claim 7, the rejection of claim 5 is incorporated and Perlman teaches:

the resource identifier further contains identifiers of certificate-issuing resources in a certification path between the trusted root resource and the resource issuing the digital certificate [Fig. 3, 5, **paragraph 0029, paragraph 0037 "a conventional certificate chain comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N)", paragraph 0050, 0051 "the root CA 14.1 may generate a collapsed certificate for the ICA 14.5 signed by the root CA 14.1 and including an indication of the identity of the ICA 14.4. Similarly, the ICA 14.4 may generate a collapsed certificate for the client 12.3 signed by the ICA 14.4 and including an indication of the identity of the ICA 14.5. Accordingly, consistent with the present invention, a collapsed certificate may be generated anywhere within a chain of linked**

certificates, in which two (2) or more linked certificates are collapsed to form a single certificate"].

As per claim 8, the rejection of claim 5 is incorporated and Benantar teaches the digital certificate is for use in a computing system **[Figs. 1, 3, 4]**. Further, Perlman teaches the digital certificate is for use in a computing system, and the certification path leads to a trusted source for the computing system **[Figs. 1-3, paragraph 0023 "The system 10 includes a plurality of entities. In this illustrative embodiment, such entities may comprise components in a computer network such as principals, clients, servers", paragraph 0024 "the system 10 includes a plurality of clients 12.1-12.N, a plurality of Certification Authorities (CA's) 14.1-14.N, a Directory Server (DS) 18 operative to provide access to certificates issued by one or more of the CA's 14", paragraph 0029 "Public Key Infrastructure (PKI) model 30, which may be deployed in the computer network 16 (see FIG. 1) to enable the discovery of public keys. Specifically, the PKI model 30 comprises a "top-down" hierarchical model that includes a single root CA 14.1, a plurality of Intermediate Certification Authorities (ICA's) 14.2-14.7, and a plurality of clients 12.1-12.4", paragraph 0030]**.

As per claim 9, it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

As per claim 10, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 11, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

As per claim 12, the rejection of claim 9 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected with the same rationale applied against claim 8 above.

As per claim 13, Benantar teaches:

a digital certificate having an authority identification field **[Fig. 5, 500]**, containing a resource identifier that contains information identifying certificate-issuing resource **[Fig. 506].** Benantar teaches the authority identification field, contains identifying information identifying each of a plurality of resources in a tree **[paragraph 0032 lines 18-22, "The distinguished name (DN) of a subject or issuer is formed by concatenating a series of relative distinguished name (RDNs) corresponding to nodes in a tree known as a directory information tree (DIT)];** identifying the certificate-issuing resource that issued the digital certificate based on the resource identifier in the authority identification field of the digital certificate **[Fig. 5, 506,**

paragraph 0032 lines 11-18 "the issuer's distinguished name 506, and the issuer's signature 508"]; querying the certificate-issuing resource to determine status of the certificate **[Fig. 3, step 316].** Benantar doesn't explicitly mention identifying *each of a plurality of certificate-issuing resources in the certification path of the digital certificate and determine if the digital certificate has been revoked*.

However, Perlman teaches: the digital certificate **[Fig. 5, 4]** contains the identifying information identifying *each of a plurality of certificate-issuing resources in a certification path of the digital certificate* **[Fig. 5, 3, paragraph 0036, "Certificate chains generated by CA's in conventional systems typically comprise certificate chains like the certificate chain 40. For example, in the event the top-down model 30 is deployed in a conventional system....", paragraph 0037, a conventional certificate chain comprising a plurality of linked certificates is converted into a collapsed certificate. FIG. 5 depicts a conceptual representation of an exemplary collapsed certificate 50 issued by a CA in response to a request by a client. In one embodiment, the collapsed certificate 50 includes an indication 52 of the identity of a CA, an indication 54 of the identity of at least one ICA (i.e., the ICA's 54.1-54.N), and an indication 56 of the identity of a client", paragraph 0051];** *determining if the digital certificate has been revoked* **[paragraph 0044 "CA's or clients may determine whether the certificate of any ICA in the chain has been revoked by testing the names of the ICA's included in the collapsed certificate against names included in a CRL..."].**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the digital certificate of Benantar's invention by including the identification information as taught by Perlman because it would reduce bandwidth utilization and processing overhead associated with the processing of linked certificates **[Perlman, paragraph 0021 lines 6-11].**

As per claim 14, the rejection of claim 13 is incorporated and it encompasses limitations that are similar to limitations of claim 6. Thus, it is rejected with the same rationale applied against claim 6 above.

As per claim 15, the rejection of claim 13 is incorporated and it encompasses limitations that are similar to limitations of claim 7. Thus, it is rejected with the same rationale applied against claim 7 above.

As per claim 16, the rejection of claim 13 is incorporated and it encompasses limitations that are similar to limitations of claim 8. Thus, it is rejected with the same rationale applied against claim 8 above.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Wray (US 2001/0014943) -- Method and apparatus for discovering a trust chain imparting a required attribute to a subject

Fatamura et al (US 2002/0073311) – Public key certificate issuance request processing system and Public key certificate issuance request processing method

Gunter et al (US 2003/0172298) -- Method and system for maintaining secure access to web server services using server-delegated permissions

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP

4/25/08

/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135